Title of paper for Artificial Intelligence (AI) in Hardware track

Using AI in fuzz testing and penetration testing for hardware security verification/validation

Author
Rachana Maitra
Senior Principal Engineer, Corporate SDL, Marvell Technology

Abstract

This paper will present some aspects of product security testing that could use artificial intelligence capabilities. Contrary to ensuring functional correctness and compliance to power and performance expectations, product security testing aims to ensure the absence of behavior or characteristics that a hacker could utilize for malicious intent such as stealing or counterfeiting IP, disrupting, or corrupting functionality, leaking secret key or other critical assets of a product. Therefore, when creating a security test plan, the test parameters or what to look for while analyzing test results must not be bounded merely by what is expected. It should assume the mindset of a hacker who may be experimenting with parameters not necessarily restricted by product specification, in attempts to find loopholes. There are two popular concepts of product security testing: Fuzz testing (techniques that involve testing with randoms, including invalid inputs to discover bugs and vulnerabilities) and Penetration testing (techniques that involve exploiting vulnerabilities, like an actual attacker). While fuzz testing could benefit from matured AI models which have been trained with in-depth internal knowledge of the product, along with exhaustive automation capabilities, penetration testing could take advantage of AI capabilities even in its infancy. Inherently, non-matured AI capabilities could better mimic real-life hackers who will attempt to break a product with whatever information is available, then continue to build on it. This paper will delve into exploring both possibilities, starting with using AI in threat modeling to analyze potential security risks of a product, followed by requirements to mitigate the risks.